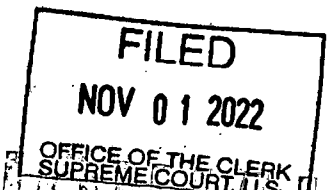
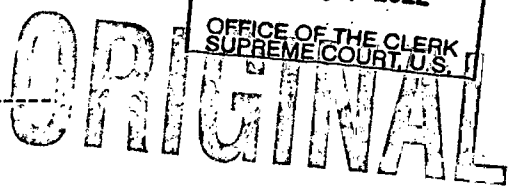
22-6026

No. _____





IN THE

SUPREME COURT OF THE UNITED STATES

Robert C. Stryker -- PETITIONER

VS.

State of Wisconsin -- RESPONDENT

ON PETITION FOR A WRIT OF CERTIORARI TO

The Wisconsin Court of Appeals

PETITION FOR WRIT OF CERTIORARI

Robert C. Stryker

Inmate #650483

New Lisbon Correctional Institution

P.O. Box 2000

New Lisbon, Wisconsin 53950-2000

QUESTIONS PRESENTED

- Were the petitioner's Fourth Amendment rights violated when the contents of computer files held in evidence against him were revealed in warrantless searches?
- Should federal courts reviewing state court decisions in criminal cases involving social worker-patient privilege apply the federal social worker privilege first described in ***Jaffee v. Redmond***, 518 U.S. 1 (1996), or should federal courts apply the state social worker-patient privilege? In petitioner's case, the state courts required a novel procedure to deny petitioner's claim that a computer file was subject to social worker-patient privilege under state law, finding petitioner's attorney was not ineffective for failing to seek its exclusion, and denying petitioner's motion to strike confidential information from the court record and publicly available documents.

LIST OF PARTIES

All parties appear in the caption of the case on the cover page.

CHRONOLOGICAL LIST OF COURT PROCEEDINGS (Page 1 of 2)

Case caption in all courts: ***State of Wisconsin v. Robert C. Stryker***
Circuit Ct. No.: 14CF1068 Appeal No.: 2021AP0692-CR

Date	Court	Proceeding (Rec. No.)
9/15/14	Cir. Ct.	Initial appearance (Tr. R117)
9/24/14	Cir. Ct.	Bail modification hearing (Tr. R118)
10/9/14	Cir. Ct.	Bail modification hearing (Tr. R119)
10/24/14	Cir. Ct.	Waiver of preliminary hearing (Tr. R120)
11/24/14	Cir. Ct.	Arraignment hearing (Tr. R121)
1/15/15	Cir. Ct.	Status hearing (Tr. R122)
5/11/15	Cir. Ct.	Motion hearing: defendant's motion to supp. (R13; Tr. R123)
6/24/15	Cir. Ct.	Oral ruling: denial of defendant's motion to supp. (Tr. R133)
7/10/15	Cir. Ct.	Bail modification hearing (Tr. R124)
8/1/15	Cir. Ct.	Judicial transfer from Hon. K. Foster to Hon. R. Ramirez
8/17/15	Cir. Ct.	Bail modification hearing (Tr. R125)
10/21/15	Cir. Ct.	Bail modification hearing (Tr. R126)
12/18/15	Cir. Ct.	Motion hearing: defendant's motion to reconsider - denied (R29; Tr. R127)
1/12/16	Cir. Ct.	Status hearing (Tr. R128)
1/14/16	Cir. Ct.	Plea hearing (Tr. R129)
2/17/16	Cir. Ct.	Bail modification hearing (Tr. R131)
5/2/16	Cir. Ct.	Scheduling conference (Tr. R132)
8/19/16	Cir. Ct.	Status hearing (Tr. R134)
9/22/16	Cir. Ct.	Bail modification hearing (Tr. R135)
12/19/16	Cir. Ct.	Sentencing hearing (Tr. R136)
3/17/17	Ct. App.	State public defender assigns Attorney M. De Peters as appellate counsel. Transcripts ordered. (R67)
2/9/18	Ct. App.	Ct. App. grants counsel's motion to extend postconviction motion or notice of appeal filing deadline by 60 days.
4/12/18	Ct. App.	Ct. App. grants counsel's motion to ext. deadline by 60 days.
6/11/18	Ct. App.	Ct. App. grants counsel's motion to ext. deadline by 60 days.
8/8/18	Ct. App.	Ct. App. grants counsel's motion to ext. deadline by 60 days.
10/12/18	Ct. App.	Ct. App. grants counsel's motion to ext. deadline by 60 days.
12/11/18	Ct. App.	Ct. App. grants counsel's motion to ext. deadline by 60 days.
2/12/19	Ct. App.	Ct. App. grants counsel's motion to ext. deadline by 60 days.
4/12/19	Ct. App.	Ct. App. grants counsel's motion to ext. deadline by 60 days.
6/10/19	Ct. App.	Ct. App. grants counsel's motion to ext. deadline by 60 days.
7/2/19	Cir. Ct.	Motion for postconviction relief filed by counsel. (R68)
8/7/19	Cir. Ct.	Scheduling conference
11/1/19	Cir. Ct.	Motion hearing: motion for postconviction relief (Tr. R137)
1/3/20	Cir. Ct.	Oral ruling: denial of motion for postconviction relief (Tr. R138)

CHRONOLOGICAL LIST OF COURT PROCEEDINGS (Page 2 of 2)

Case caption in all courts: ***State of Wisconsin v. Robert C. Stryker***
Circuit Ct. No.: 14CF1068 Appeal No.: 2021AP0692-CR

Date	Court	Proceeding (Rec. No.)
1/8/20	Ct. App.	Counsel files notice of appeal. (R75)
6/3/20	Ct. App.	Ct. App. grants defendant's motion to dismiss counsel. (R82)
7/15/20	Cir. Ct.	Second motion for postconviction relief filed by (pro se) defendant. (R83)
8/12/20	Cir. Ct.	Circuit court partly denies second motion for postconviction relief.
9/18/20	Cir. Ct.	Amended motion for postconviction relief filed by (pro se) defendant. (R88)
10/8/20	Cir. Ct.	Status conference
12/10/20	Cir. Ct.	Motion to destroy confidential information (in court records) filed by (pro se) defendant. (R94)
12/11/20	Cir. Ct.	Circuit court denies motion to destroy confidential information. (R95)
1/8/21	Cir. Ct.	Motions to seal/redact court records and transcripts filed by (pro se) defendant. (R96 & R97)
3/26/21	Cir. Ct.	Oral ruling: denial of defendant's amended second motion for postconviction relief, denial of defendant's motion to seal/redact transcripts, and partial denial and partial granting of defendant's motion to seal/redact a court record. (R115; Tr. R139)
4/16/21	Ct. App.	(Pro se) defendant files notice of appeal. (R111)
6/23/21	Ct. App.	(Pro se) defendant files brief-in-chief.
9/7/21	Ct. App.	State files response brief.
9/29/21	Ct. App.	(Pro se) defendant files reply brief.
6/1/22	Ct. App.	Ct. App. issues decision affirming defendant's conviction.
6/6/22	Ct. App.	(Pro se) defendant files Motion for Reconsideration and Motion to Remove Confidential Information from Ct. App. Decision.
6/10/22	Ct. App.	Ct. App. denies both post-decision motions.
6/29/22	Wis. S.C.	(Pro se) defendant files petition for review with Wisconsin Supreme Court.
9/13/22	Wis. S.C.	Wisconsin Supreme Court denies petition for review.

Notes: 1. No docket numbers are available for filings with the court of appeals and Wisconsin Supreme Court.

2. If a record no. ("R#") appears for a filing with the court of appeals, the record number refers to a duplicate document filed with the circuit court.

3. "Tr." indicates transcripts for the proceeding filed in court record.

TABLE OF CONTENTS (Page 1 of 2)

TABLE OF CONTENTS (Page 2 of 2)

Appendix--Table of Contents

TABLE OF AUTHORITIES (Page 1 of 6)

AUTHORITY **PAGE(S)**

Federal Cases (continued)

AUTHORITY — **PAGE(S)**

Federal Cases (continued)

AUTHORITY **PAGE(S)**

Federal Cases (continued)

AUTHORITY **PAGE(S)**

Other State Authorities

IN THE

SUPREME COURT OF THE UNITED STATES

PETITION FOR WRIT OF CERTIORARI

Petitioner respectfully prays that a writ of certiorari issue to review the judgment below.

OPINIONS BELOW

For cases from **state courts:**

The opinion of the highest state court to review the merits (Wisconsin court of appeals) appears at Appendix A to the petition and is unpublished: ***State v. Stryker***, No. 2021AP0692-CR, 2022 WL 1772243 (Wis. Ct. App. Jun. 1, 2022).

The following opinions of the Waukesha County circuit court appear in Appendix B and are unpublished:

- B01-B20 June 24, 2015 oral ruling for first pretrial motion to suppress (pp. 1-20);
- B21-B28 December 18, 2015 oral ruling for motion to reconsider (pp. 1, 25-31);
- B29-B47 January 3, 2020 oral ruling for first postconviction motion (pp. 1, 45-62);
- B48-B83 March 26, 2021 oral ruling for second postconviction motion (pp. 1-36).

JURISDICTION

For cases from **state courts:**

The date on which the highest state court (Wisconsin Supreme Court) decided petitioner's case was September 13, 2022. A copy of that decision (one-page denial of review) appears at Appendix C.

The jurisdiction of this Court is invoked under 28 U. S. C. § 1257(a).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

This case involves the following amendments to the United States Constitution and federal and Wisconsin statutes, of which the relevant parts are included in Appendix D:

- Fourth Amendment to the United States Constitution.
- Fourteenth Amendment to the United States Constitution.
- The federal social worker-patient privilege established in ***Jaffee v. Redmond***, 518 U.S. 1 (1996) through Federal Rule of Evidence 501.
- Wisconsin's statute governing pretrial motions to suppress evidence in Wis. Stat. § 971.31(10).
- Wisconsin's social worker-patient (and marriage and family therapist) privilege in Wis. Stat. § 905.04.
- Wisconsin's statute covering self-authentication of certain types of evidence, Wis. Stat. § 909.02.
- Wisconsin's statute governing some hearsay exceptions, Wis. Stat. § 908.03, which is referenced in Wis. Stat. § 909.02.
- Wisconsin's statute defining health care records, Wis. Stat. § 146.81, which is referenced in Wis. Stat. § 908.03.

STATEMENT OF THE CASE

This case involves warrantless searches of files on Robert C. Stryker's (petitioner's) computer performed by the police under the auspices of third party consent of the petitioner's wife.

On August 29, 2014, the police spoke with petitioner's estranged wife who had filed for divorce about six weeks previously (R123:11, 15). She reported that in 2010, petitioner had admitted to her that he had viewed child pornography (R123:7, 34). The police did not get a search warrant but instead obtained consent to search petitioner's computer from her (R123:41-43, 49-50).

A police detective conducted a forensic analysis of petitioner's computer and found evidence consisting of 64 thumbnail-sized, hidden images of child pornography which were inaccessible without forensic software (R123:79-81), a deleted, password-protected Microsoft Word file, Inventory.doc, which was an autobiography of petitioner and focused on his sexual history (R123:61 & R127:9-10), and some system files indicating programs and files used (R1:6-7). Based on this evidence, petitioner was arrested on September 13, 2014 and charged with five counts of possession of child pornography on or about August 27, 2014 (R1:1-3).

A. Motion to Suppress Fruits of Unlawful Search and Seizure.

Trial counsel filed a pretrial motion to suppress the search of the files on petitioner's computer (R13). In the motion, petitioner argued his wife did not "have mutual use of the computer folder and files on a computer which she never used," that she did not "generally ha[ve] joint access or control of those files for most purposes," and that therefore she did not

have "the authority to permit law enforcement's inspection of those files" (R13:1). A hearing was held in front of Judge Foster on May 11, 2015. Petitioner's wife testified that:

- Petitioner had voluntarily told her he had viewed child pornography and had started counseling in 2010 (R123:7). She "never did work with files" on petitioner's laptop (R123:8-9, 24-25). She never saw anything concerning on petitioner's computer (R123:17, 20-21). She was not aware of the existence of Inventory.doc until April 2015 and the police never asked her questions about it (R123:27-28).

Two police officers testified that:

- They obtained permission from petitioner's wife to search petitioner's computer--a warrant was never obtained (R123:42-43, 50). Petitioner's wife had told police "she had never gone on the laptop" (R123:49).
- There was no password required to log onto the computer, but one file, "a Word document which appeared to be an autobiography of [petitioner] in regards to some personal issues," which was "called Inventory," did require a password (R123:60-61). A 19-page report was created from the forensic analysis of petitioner's computer (R123:64) which showed that none of the 64 images had any created, modified, or accessed dates associated with them (R17:3-21). Manual analysis revealed 64 images of suspected child pornography (R123:67): 52 were hidden thumbcache images which were generated by the operating system and the remaining 12 were hidden carved (deleted) images; forensic software was needed to find and view all 64 images (R123:76, 79-81). "Windows by default hides thumbcaches and other file systems that it needs to operate so [the average

user] can't access them," (R123:79-80). Petitioner's computer did not have software necessary to view the file names or the images themselves (R123:89).

- Neither detective talked to petitioner's wife to get the password to access Inventory.doc; someone else did but neither detective knew who. She provided a list of possible passwords; the exact password was not remembered by the detectives, and neither detective documented any of this (R123:56, 82-83).

The trial court denied petitioner's motion in its entirety on June 24, 2015 (App:B01-B20).

B. Defendant's Motion to Reconsider

Trial counsel filed a motion to reconsider (R29), and a hearing was held in front of Judge Ramirez on December 18, 2015. One of the detectives testified again and gave divergent testimony. He now admitted he used the forensic software to undelete Inventory.doc (he did not previously acknowledge that Inventory.doc was deleted) and then said he called petitioner's wife directly for a list of possible passwords; the one that worked had something to do with the Brewers, but he remembered no more specifics about it (R127:9-11) and did not document any of this (R127:13). The trial court denied the motion in its entirety (App:B21-B28).

C. Plea hearing and sentencing hearing.

Petitioner pled guilty to an amended charge of one count of possession of child pornography with an offense date of January 2010 (R129:2-14). At the plea hearing, trial counsel pointed out that the amended information to which petitioner pled guilty was based on Inventory.doc (R129:9-10).

The State filed Inventory.doc on the record prior to the sentencing hearing (R55:4-12). At the sentencing hearing, both the prosecutor and trial counsel recognized Inventory.doc as a treatment document (R136:9-10, 25-26). In December 2016, petitioner was sentenced to eight years of incarceration followed by eight years of extended supervision (concurrent with an identical sentence from a conviction in 15CF0985) (R136:41). Trial counsel timely filed an intent to pursue postconviction relief (R62).

D. First postconviction motion and subsequent hearings.

Appointed appellate counsel filed the first postconviction motion in this case with the circuit court on July 2, 2019 (R68 & R69), arguing the trial court erroneously exercised its discretion in finding the search of petitioner's computer complied with the Fourth Amendment and also claimed trial counsel was ineffective in not seeking exclusion of Inventory.doc under Wisconsin's social worker-patient privilege statute. (In Wisconsin, a defendant maintains the right to challenge the denial of a motion to suppress even after pleading guilty. Wis. Stat. § 971.31(10).)

A hearing pursuant to ***State v. Machner***, 92 Wis. 2d 797, 285 N.W.2d 905 (Ct. App. 1979) was held on November 1, 2019 during which petitioner's trial counsel testified that not seeking exclusion of Inventory.doc under Wis. Stat. § 905.04 was an oversight and again identified the document as something petitioner produced as part of his therapy (R137:13, 32).

At the postconviction hearing on January 3, 2020, in its decision regarding the issues related to the pretrial motions to suppress, the circuit court (Judge Dorow) simply read the previous trial court decisions into the record, adopting them as its own decision, without analysis (App:B35-B36, B39-B41). The circuit court also found petitioner's trial counsel was not ineffective,

deciding that Inventory.doc was not subject to privilege under Wis. Stat. § 905.04 because the argument was inadequate (App:B46-B47).

E. Second postconviction motion and petitioner's motions to keep contents of Inventory.doc confidential.

Postconviction counsel timely filed a Notice of Appeal (R75). Petitioner subsequently dismissed counsel in favor of proceeding pro se, asked the appellate court to dismiss the appeal, and, after the circuit court partially denied his second postconviction motion, filed an amended second postconviction motion on September 18, 2020 (R88). Petitioner again argued the trial court erroneously exercised its discretion in finding the search of his computer complied with the Fourth Amendment and again argued that he should be allowed to withdraw his guilty plea because he was denied his right to effective assistance of counsel when his trial counsel failed to argue that Inventory.doc was subject to social worker-patient privilege under Wis. Stat. § 905.04. Petitioner obtained a notarized affidavit from his social worker attesting to Inventory.doc's status as a treatment document (App:I01) and also provided a thorough analysis of Wis. Stat. § 905.04 as it pertained to the facts of his case (R88:11-12).

Before the circuit court decided his second postconviction motion, petitioner filed a "Motion to Destroy Confidential Information" on December 10, 2020 (App:E01-E03), which the circuit court denied without a hearing (App:F01); he subsequently filed a "Motion to Seal or Redact a Transcript" (App:G01-G03) and a "Motion to Seal or Redact a Court Record" (App:H01-H05).

At a March 26, 2021 hearing, the circuit court denied the second postconviction motion, denied reconsideration of the Motion to Destroy Confidential Information, and denied the two

motions to seal or redact, except the court agreed to seal the actual text of Inventory.doc. In regards to the Fourth Amendment claim, the circuit court read the previous decisions into the record without further analysis and it denied petitioner's ineffective assistance of counsel claim because--in sua sponte rationale--neither petitioner nor his social worker testified to authenticate Inventory.doc (App:B48-B83).

F. Petitioner's arguments to court of appeals.

Petitioner filed a pro se brief in the court of appeals on June 23, 2021.

1. Search violating the Fourth Amendment.

Petitioner, in his appellate brief, first cited state and federal decisions (***United States v. Matlock***, 415 U.S. 164, 171 n.7 (1974); ***Illinois v. Rodriguez***, 497 U.S. 177, 181 (1990)) to establish the authority of a third party to provide general consent to search under the Fourth Amendment (Pet. Br. 15). He then cited ***Rakas v. Illinois***, 439 U.S. 128, 144 n.12 (1978) and ***Georgia v. Randolph***, 547 U.S. 103, 111 (2006) in arguing that societal expectations of privacy need to be considered when determining Fourth Amendment reasonableness in third-party consent cases (Pet. Br. 15). Petitioner then cited ***Trulock v. Freeh***, 275 F.3d 391, 403 (4th Cir. 2001) and a state decision in arguing that a third party's authority to consent to a search of electronic files was predicated upon the third party's mutual use of the files through joint access or control for most purposes (Pet. Br. 16).

Petitioner asserted that individual files each represent a separate search, citing several persuasive authorities, and therefore the characteristics of each file need to be considered when evaluating a defendant's motion to suppress (Pet. Br. 16-17).

Petitioner claimed his wife did not have authority over any of the files held in evidence against him because they were all inaccessible to her (Pet. Br. 17-18). He then claimed she did not have authority over the file Inventory.doc specifically for three different reasons:

- The State failed to prove by clear and convincing evidence that she provided the police with the exact password to Inventory.doc (Pet. Br. 18-20).
- Inventory.doc was deleted and was inaccessible to her (Pet. Br. 21).
- Petitioner had an expectation of privacy in Inventory.doc that society would recognize (Pet. Br. 21-22).

Petitioner then argued the circuit courts' errors in failing to suppress the files were not harmless (Pet. Br. 22-23).

The court of appeals affirmed the circuit courts' rulings, finding that petitioner's wife's authority to have the laptop searched superseded any access issues or personal privacy issues with any individual files (App:A13-A16).

2. Ineffective assistance of counsel claim predicated on privileged nature of Inventory.doc.

In petitioner's appellate brief, he discussed relevant state and federal case law (***Strickland v. Washington***, 466 U.S. 668 (1984)) regarding a claim of ineffective assistance of counsel in the context of postconviction plea withdrawal (Pt. Br. 23-24). He then argued that the circuit court erroneously found that (1) petitioner failed to show Inventory.doc was a privileged document under Wis. Stat. § 905.04, and (2) trial counsel's performance wasn't deficient (Pet. Br. 24-25). Petitioner then went through his argument establishing that trial counsel's performance was deficient because Inventory.doc was privileged (Pet. Br. 26-27), following that with the assertion

that this deficient performance was prejudicial because petitioner would have otherwise proceeded to trial (Pet. Br. 27-28).

Petitioner later identified a supplemental authority, ***State v. Burch***, 2021 WI 68, ¶27, 398 Wis. 2d 1, 961 N.W.2d 314, which bolstered his argument (App:J01-J02).

The court of appeals affirmed the circuit court's ruling that petitioner had failed to prove that Inventory.doc was privileged under Wis. Stat. § 905.04 and provided no further analysis (App:A17-A18).

Petitioner subsequently submitted a Motion for Reconsideration to the court of appeals (App:K01-K03) in which he argued the circuit court's requirement of live testimony to authenticate Inventory.doc as a medically privileged document under Wis. Stat. § 905.04 was statutorily barred. The court of appeals denied petitioner's motion without analysis (App:A19).

3. Removal of confidential information predicated on privileged nature of Inventory.doc.

In his appellate brief, petitioner cited ***State v. Stanley***, 2012 WI App 42, ¶29, 340 Wis.2d 663, 814 N.W.2d 867, to support his claim that portions of court proceedings which are confidential per state statutes are not available for public inspection (Pet. Br. 29). He then repeated his argument that Inventory.doc was a privileged communication under Wis. Stat. § 905.04 and asserted the information should at least be put under seal in the court record, even if it isn't stricken entirely (Pet. Br. 29-30).

The court of appeals affirmed the circuit court's denial of petitioner's Motion to Destroy Confidential Information (App:E01-E03 and F01) in a footnote because petitioner had failed to prove that Inventory.doc was privileged under Wis. Stat. § 905.04 (App:A19).

4. Removal of confidential information from court of appeals' decision.

Petitioner submitted a post-decision "Motion for Removal of Confidential and Privileged Information from Court of Appeals' Decision," (App:L01-L03) seeking removal of one sentence from the decision. His motion applied all relevant elements of Wis. Stat. § 905.04 to the facts regarding the sentence. The court of appeals immediately denied petitioner's motion without analysis (App:A19).

G. Wisconsin Supreme Court

Petitioner filed petition for review with the Wisconsin Supreme Court on June 29, 2022, which was denied on September 13, 2022 (App:C01).

REASONS FOR GRANTING THE WRIT

In the petitioner's case, the police used his divorcing wife's consent to conduct a warrantless search of his laptop computer. Every file used against the petitioner was unknown and inaccessible to her, including one prepared by the petitioner as part of his voluntary mental health treatment with a social worker, but because the inaccessible files were in electronic format on a computer and not paper files in a locked file cabinet, the government has been able to circumvent:

- the third party consent doctrine established in ***Matlock***, 415 U.S. at 171, n.7;
- societal privacy expectations outlined in ***Rakas***, 439 U.S. at 143, n.12 and ***Randolph***, 547 U.S. at 111;
- social worker-patient privilege established in Wis. Stat. § 905.04.

The petitioner's case presents an opportunity for the U.S. Supreme Court to define something with which lower courts have been struggling for decades: how does the third party consent exception to the warrant requirement apply to searches of media containing electronically stored information (ESI)? Additionally, the Court can answer whether the federal social worker-patient privilege established in ***Jaffee***, 518 U.S. at 15, or state statutory privilege should apply in federal courts when a federal court has jurisdiction to decide the matter.

A. Warrantless third party consent searches of media containing ESI.

1. Dozens of these searches occur each year.

How often are warrantless third party consent searches of media containing ESI conducted? A thorough review of federal and state court decisions in Westlaw from calendar year 2021

identified 14 decisions involving third party consent searches of media containing ESI (see Appendix M). Assuming that for every case involving such a search appearing in the Westlaw database, there was another one not in the database because the search was not challenged on appeal, a reasonable estimate is a couple dozen such searches occur every year. Undoubtedly, there have been hundreds of warrantless third party consent searches of media containing ESI performed in the past few decades. This is not an unusual circumstance by any measure.

2. How have courts applied the third party consent doctrine to warrantless searches of media containing ESI?

a. The U.S. Supreme Court has not directly addressed this issue.

This Court first broached the subject of warrantless, third party consent searches in ***Chapman v. United States***, finding that a landlord could not validly consent to the search of a house he had rented to the target of the search. 365 U.S. 610, 616-18 (1961). A few years later, the Court similarly decided that a night hotel clerk could not validly consent to a search of a customer's room. ***Stoner v. California***, 376 U.S. 483, 490 (1964). This Court considered the authority of a third party to consent to the search of an object in ***Frazer v. Cupp***, finding that the cousin of the search target could consent to the search of a duffel bag they jointly used and which was located at the cousin's residence. 394 U.S. 731, 740 (1969). Two years later, the Court decided that no search or seizure had occurred when the search target's wife turned over his guns and clothing to police without being asked to do so. ***Coolidge v. New Hampshire***, 403 U.S. 443, 489-90 (1971).

In ***Schneckloth v. Bustamonte***, this Court found that a third party could consent to the search of a car in which stolen checks implicating the defendant were found, and voluntariness of

consent did not require the consenter's knowledge that he could refuse. 412 U.S. 218, 248-49 (1973). The following year, the Court found that a girlfriend who cohabitated with the search target could consent to the search of a shared bedroom, and in doing so, explained how the third party's authority to consent should be evaluated:

> [W]hen the prosecution seeks to justify a warrantless search by proof of voluntary consent, it is not limited to proof that consent was given by the defendant, but may show that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected.[Footnote 7]
>
> ...
>
> [Footnote 7]: ... The authority which justifies the third-party consent does not rest upon the law of property, ... but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

Matlock, 415 U.S. at 171, n.7.

The Court later introduced the concept of "apparent authority," holding that police can rely on apparent authority of a third party, who asserts she is a resident, to search the premises even if later they learn she is not a resident. ***Rodriguez***, 497 U.S. at 188-89. In ***Randolph***, this Court held that police could not rely on the consent of a third party to conduct a warrantless search of a residence if the search target is physically present and objects to the search. 547 U.S. at 120. The Court later found that the search target must be physically present and objecting to the search at the same time in order to overcome the third party's authority to consent to a search of the residence. ***Fernandez v. California***, 571 U.S. 292, 302-06 (2014).

This Court has issued two decisions regarding warrantless searches of media containing ESI. In ***Riley v. California***, the Court found that the incident to arrest exception could not generally be used to conduct a warrantless search of a cell phone, and heightened interests in the

privacy of digital data were cited as a main concern. 573 U.S. 373, 403 (2014). Later, the Court held that generally, the government must secure a search warrant, supported by probable cause, before obtaining cell-site location information from a wireless carrier. ***Carpenter v. United States***, 138 S. Ct. 2206, 2221 (2018).

Finally, one other recent decision of this Court is relevant to the petitioner's case. The Court found that an individual could be authorized to access a computer in general, but would exceed his authority if he "obtains information located in particular areas of the computer--such as files, folders, or databases--that are off limits to him." ***Van Buren v. United States***, 141 S. Ct. 1648, 1662 (2021).

The bottom line is this: all lower court rulings allowing warrantless, third party consent searches of media containing ESI are extrapolations of (1) a 1969 decision by this Court establishing the authority of a third party to consent to a search of a jointly-used duffel bag--that is the lone object covered by these decisions--and (2) several decisions involving a third party's authority to consent to a search of a residence or automobile.

b. Lower courts have inconsistently applied the doctrine to warrantless searches of media containing ESI.

Warrantless third party consent searches of media containing ESI first appeared in appellate cases over twenty years ago, and two of the earliest cases provide an example of forthcoming inconsistency in decisions: one court found a third party has authority to consent to the search of a shared computer when the third party has complete access to the computer, ***United States v. Smith***, 27 F.Supp.2d 1111 (C.D. Ill. 1998), and another court found that a computer repair

technician did not have authority to consent to a search of the defendant's computer, ***United States v. Barth***, 26 F.Supp.2d 929 (W.D. Tex. 1998).

Shortly thereafter, the Fourth Circuit provided a well-reasoned analysis of individual file characteristics in consideration of a third party's authority by referencing ***Matlock***:

> Authority to consent originates not from a mere property interest, but instead from "mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that others have assumed the risk that one of their number might permit the common area to be searched." ***United States v. Matlock***, 415 U.S. 164, 171 n. 7, 94 S.Ct. 988, 39 L.Ed.2d 242 (1974)...
>
> We conclude that, based on the facts in the complaint, [the third party] lacked authority to consent to the search of Trulock's files. [The third party] and Trulock both used a computer located in [the third party's] bedroom and each had joint access to the hard drive. [The third party] and Trulock, however, protected their personal files with passwords; [the third party] did not have access to Trulock's passwords. Although [the third party] had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files...

Trulock, 275 F.3d at 403. Many subsequent cases cited ***Trulock*** but misstated its holding, claiming that a search target must affirmatively take action to block access to a third party or else he has forfeited any privacy expectation in ESI:

- ***United States v. Aaron***, 33 Fed. Appx. 180, 184 (6th Cir. 2002) ("In the personal computer context, courts examine whether the relevant files were password-protected or whether the defendant otherwise manifested an intention to restrict third-party access. ***Trulock v. Freeh***, 275 F.3d 391, 403 (4th Cir. 2001)");
- ***United States v. Rader***, 65 M.J. 30, 34 (C.A.A.F. 2007) (citing ***Aaron*** above);
- ***United States v. Sager***, No. 3:07-CR-80(01)RM, 2008 WL 45358 (N.D. Ind. Jan. 2, 2008) ("A password unknown to the third party may defeat a claim of apparent authority over the contents of a password-protected computer, see, e.g., ***Trulock v. Freeh***, 275 F.3d

391, 403 (4th Cir.2001), but no password was needed to gain access to the pertinent images on the basement computer.");

See also ***State v. Aschinger***, 232 P.3d 831, 836 (Ct. App. Ida. 2009); ***United States v. Trejo***, 471 Fed.Appx. 442 (6th Cir. 2012).

The concurrence portion of Judge Michael's opinion in ***Trulock*** explains why this misconception is wrong: "Knowledge of the passwords is necessary, but not sufficient, to establish common authority over password-protected files. The third party must also have 'joint access' to the files 'for most purposes.' ***Matlock***, 415 U.S. at 171 n. 7, 94 S.Ct. 988." ***Trulock***, 275 F.3d at 408 n. 1 (Michael, J., concurring in part and dissenting in part). Hence, while password protection is a means to achieve third party inaccessibility, files which are not password-protected are not automatically fair game. The third party must also have "mutual use of the" files by generally having "joint access or control for most purposes." ***Id.***, 275 F.3d at 403.

This confusion pervades to this day. In a very recent case, a military judge ruled that a third party had no authority over another's cell phone beyond "texting, calling, viewing YouTube, and playing games"--even though the ESI implicating the defendant was technically accessible to the third party; the military judge's ruling was reversed on an interlocutory appeal by the U.S. Army Court of Criminal Appeals (***United States v. Black***, No. ARMY Misc. 20210310, 2021 WL 4953849, at *5, *8 (A. Ct. Crim. App. Oct. 22, 2021) (unpublished)). The appellate decision was reversed a few months ago and the original military judge's order upholding the suppression motion reinstated:

> Neither the Supreme Court nor this Court has ever held that the scope of a person's common authority over property is coextensive with that person's access to the property. If that were true, determining whether common authority existed would be trivial....

> In ***United States v. Rader***, this Court expressly rejected the idea that the owner of a computer that was also used by a third party could not limit the scope of the third party's access to certain applications or files. 65 M.J. 30, 34 (C.A.A.F. 2007). And although the Court recognized that one way of restricting access was through the use of technological restraints such as passwords or encryption, we also acknowledged that courts should consider "whether the defendant otherwise manifested an intention to restrict third-party access." ***Id.*** (internal quotation marks omitted) (citation omitted). Accordingly, even though Appellant had not password protected or encrypted the photo galleries containing the child pornography, that does not mean that Appellant could not have excluded those galleries from the scope of PFC Avery's common authority.

United States v. Black, --- M.J. ----, Appeal No. 22-0066, 2022 WL 3724125, *4 (C.A.A.F. 2022).

However, there was a dissenting judge agreeing with the lower court's reversal. "I cannot help but conclude that Appellant allowed [the third party] joint access and control and therefore assumed the risks involved with lending his cell phone and its illegal contents." ***Black***, --- M.J. ---, Appeal No. 22-0066, 2022 WL 3724125 at *9 (Sparks, J., dissenting).

In summation, there is no consensus after nearly a quarter century of appellate decisions regarding warrantless third party consent searches of media containing ESI. The 2022 ***Black*** decision contains the same disparate conclusions reached in the 1998 ***Smith*** and ***Barth*** decisions. Only Supreme Court review can resolve this longstanding conflict in the lower courts.

c. Apparent authority is often applied to warrantless searches of media containing ESI.

Another issue clouding warrantless third party consent searches of media containing ESI is "apparent authority," wherein suppression of evidence obtained in violation of a search target's Fourth Amendment rights is deemed unnecessary if "the facts available to the officer at the moment [of the search] warrant a man of reasonable caution in the belief that the consenting party had authority over the premises." ***Rodriguez***, 497 U.S. at 188 (internal citations omitted). Apparent authority has been applied in many of these lower court decisions:

- ***United States v. Buckner***, 473 F.3d 551, 553 n.1, 555 n.3 (4th Cir. 2007) (Buckner's files were password-protected, but "there [wasn't] any contention that the police officers deliberately used software that would avoid discovery of any existing passwords," and the court did "not hold that the officers could rely upon apparent authority to search while simultaneously using mirroring or other technology to intentionally avoid discovery of password or encryption protection put in place by the user.");

- ***United States v. Andrus***, 483 F.3d 711, 714 n.1, 720 (10th Cir. 2007) (Andrus' files were password-protected, but "[i]f the circumstances reasonably indicated [the third party] had mutual use of or control over the computer, the officers were under no obligation to ask clarifying questions," and "the officers' belief in [the third party's] authority was reasonable.");

See also ***Trejo***, 471 Fed.Appx. at 448. These cases expose problems with application of the apparent authority doctrine to warrantless third party consent searches of media containing ESI:

- Forensic software has the ability to bypass password protection and search millions of files in a matter of minutes or hours which the consenting third party could never do;

- The government has the ability to plead ignorance regarding security measures put in place by the target of the search;

- The third party can simply lie about having access and the government has no requirement to probe further.

Judge McKay's dissent in ***Andrus*** is instructive here:

> The unconstrained ability of law enforcement to use forensic software... to bypass password protection without first determining whether such passwords have been enabled

> does not "exacerbate" [the difficulty with seeing a lock on computer data], ante at 719 n. 5; rather, it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process. Indeed, the majority concedes that if such protection were "shown to be commonplace, law enforcement's use of forensic software ... may well be subject to question." Ante at 722 n. 8. But the fact that a computer password "lock" may not be immediately visible does not render it unlocked.

Andrus, 483 F.3d at 723 (McKay, J., dissenting).

Supreme Court review can address whether apparent authority doctrine can survive scrutiny in the context of warrantless third party consent searches of media containing ESI.

3. Each file represents a separate search.

Another important concept is the determination of what constitutes a search: the media containing ESI or the individual files themselves? This determination is critical; in the petitioner's case, the Wisconsin court of appeals found the third party's alleged authority over the entire computer rendered any characteristics of individual files irrelevant, contravening ***Trulock*** and its progeny. More recent opinions seem to be converging to a consensus that individual files (or at least categories of file types) each represent a separate search, but outliers like petitioner's case exist.

a. Some decisions have evaluated media containing ESI as a single container.

Some decisions, many of them older, have analogized a device containing ESI to a single container:

- ***United States v. David***, 756 F.Supp. 1385, 1390 (D. Nev. 1991) (finding a computer memo book "indistinguishable from any other closed container");
- ***United States v. Chan,*** 830 F.Supp. 531, 534 (N.D. Cal. 1993) (finding that a pager is analogous to a closed container);

- ***United States v. Ortiz***, 84 F.3d 977, 984 (7th Cir. 1996) (following ***Chan*** in holding that a pager is a closed container);

- ***United States v. Cotterman***, 709 F.3d 952, 976 (9th Cir. 2013) (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment) (rejecting the majority's split with the Fourth Circuit which found "electronic devices are like any other container that the Supreme Court has held may be searched at the border without reasonable suspicion" in ***United States v. Ickes***, 393 F.3d 501, 503–07 (4th Cir.2005)).

See also ***United States v. Finley***, 477 F.3d 250, 259-60 (5th Cir. 2007).

Other decisions have specifically rejected the notion that one device can be considered a "container":

- ***State v. Smith***, 124 Ohio St.3d 163, 168 (2009) (listing cases classifying electronic devices as closed containers but ultimately rejecting that categorization because these decisions fail "to consider the Supreme Court's definition of 'container' in [***New York v. Belton***, 453 U.S. 454, 460, (1981)], which implies that the container must actually have a physical object within it.");

- ***Schlossberg v. Solesbee***, 844 F.Supp.2d 1165, 1169 (D. Or. 2012) ("Consideration of an electronic device as a 'container' is problematic. Electronic devices do not store physical objects which are in plain view once the containers are opened. Moreover, the storage capability of an electronic device is not limited by physical size as a container is.").

- ***Riley***, 573 U.S. at 397 ("Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter.").

See also ***United States v. Waddell***, 840 Fed.Appx. 421, 433 (11th Cir. 2020); ***Burch***, 398 Wis. 2d 1 at ¶52 (Rebecca Grassl Bradley, J. (concurring)).

b. Many decisions specifically identify each file as a separate search.

Examples of authorities asserting or implying files are individual searches include the following:

- ***United States v. Forrester***, 512 F.3d 500, 511 (9th Cir. 2008) (Likening email to physical mail as both having a visible outside address not deserving of Fourth Amendment protection, but having contents which do.);
- ***United States v. Wicks***, 73 M.J. 93, 99 (C.A.A.F. 2014) ("Modern cell phones ... serve as an electronic repository of a vast amount of data akin to the sorts of personal 'papers [] and effects' the Fourth Amendment was and is intended to protect. 'The papers we create and maintain not only in physical but in digital form reflect our most private thoughts and activities.' ***United States v. Cotterman***, 709 F.3d 952, 957 (9th Cir. 2013)");
- ***Van Buren***, 141 S. Ct. at 1662 (This Court found that a person's authority might not extend to some files or folders even though he had authority to use a computer.).

See also ***Burch***, 398 Wis. 2d 1 at ¶38.

The most elaborate explanation of ESI files (and folders) each representing a separate search can be found in ***United States v. Stabile***, No. 08–145(SRC), 2009 WL 8641715 at *8 (D. N.J. Jan. 21, 2009):

> [T]he Court addresses the question of whether [the detective]'s opening of the Kazvid folder ... and the files located therein ... constituted searches within the meaning of the Fourth Amendment. The answer is clearly yes. See ***Arizona v. Hicks***, 480 U.S. 321, 325 ... (1987); ***United States v. Carey***, 172 F.3d 1268, 1273–74 (10th 1999) (holding

that opening computer files constitutes a search); ***United States v. Stierhoff***, 477 F.Supp.2d 423, 443–44 (D. R.I. 2007) (holding that opening computer folder constitutes a search). The Court states, for the sake of clarity, that each operation in which a folder or file was opened-that is, was highlighted, clicked or otherwise manipulated so that its contents went from being unseen to exposed-constituted a separate search. Exposing to view concealed portions of a space in which one may be authorized to search constitutes an independent search from the initial invasion and must be validly supported by a warrant or, alternatively, by an exception to the warrant requirement. ***Hicks***, 480 U.S. at 325. "Under the traditional approach, the term 'search' is said to imply some exploratory investigation, or and invasion and quest, a looking for or seeking out." ***Stierhoff***, 477 F.Supp.2d at 444 ...

c. Warrants circumscribing searches of media containing ESI imply each file is a search.

Search warrants issued for media containing ESI are very particular in describing the specific data to be searched:

- ***Carey***, 172 F.3d at 1272-73, 1276 ("The warrant ... permitted only the search of the computer files for 'names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.'... [The d]etective ... exceeded the scope of the warrant in this case. His seizure of the evidence upon which the charge of conviction was based was a consequence of an unconstitutional general search.");

- ***United States v. Flores***, 802 F.3d 1028, 1045 (9th Cir. 2015) (requiring a warrant "specify the particular crime for which the evidence is sought," rejecting retainment of unresponsive ESI under the plain view doctrine, and cautioning against "over-seizing" ESI to prevent targeted search "from turning into a general dragnet.");

- ***United States v. Harmon***, No. 3:18-cr-221-SI, 2018 WL 5786217, at *1 (D. Or. Nov. 5, 2018) ("The Ninth Circuit does not require that warrants for digital storage media specify a particular search protocol ... but law enforcement officers are 'always limited by the longstanding principle that a duly issued warrant ... may not be used to engage in a

general exploratory search.' ") (quoting ***United States v. Hill***, 459 F.3d 966, 978 (9th Cir. 2006)).

See also ***United States v. Mann***, 592 F.3d 779, 782 (7th Cir. 2010); ***United States v. Comprehensive Drug Testing, Inc.***, 621 F.3d 1162, 1166, 1178 (9th Cir. 2010). The courts in all of these decisions stressed caution in the issuance and execution of search warrants for media containing ESI to prevent the equivalent of a general search from occurring.

4. Warrantless third party consent searches of media containing ESI can compromise privileged information.

An issue with permitting blanket third party consent searches of electronic media is the government's ability to circumvent privileges. Consider the hypothetical situation where a husband divulges to his wife that he has sold illegal street drugs on numerous occasions. In Wisconsin, he maintains privileges against her testifying to this fact in court, Wis. Stat. § 905.05, and against this information being used in an affidavit in support of a search warrant. ***Muetze v. State***, 73 Wis.2d 117, 130, 243 N.W.2d 393 (1976). But if the husband were to type, "I have sold illegal street drugs on numerous occasions," and save it as "drugs.doc" on his computer, and his wife gives police consent to search his computer, they can use "drugs.doc" against him. He hasn't given anyone besides his wife access to drugs.doc, but because he "ha[s] assumed the risk that [she] might permit the common area to be searched [by police]," ***Matlock***, 415 U.S. at 171, n.7, then the police can do an end run around marital privilege.

This lack of protection for privileges is highlighted when these warrantless searches are compared with searches authorized by a court through a subpoena or warrant. A court can quash a subpoena when compliance would destroy a valid privilege. ***United States v. Bergeson***, 425

F.3d 1221, 1225 (9th Cir. 2005). And as described earlier, warrants can be very specific regarding items to be seized, and a special master can be appointed to protect a search target's potentially privileged information. ***United States v. Vepuri***, --- F.Supp.3d ----, No. 21-mj-1220, 2022 WL 3648184, at *1 (E.D. Penn. Aug. 24, 2022); *see also* ***United States v. Stewart***, Case No. 02-CR-395 (JGK), 2002 WL 1300059, at *7, *10 (S.D. N.Y. Jun. 11, 2002). No such limitation exists when warrantless third party consent searches of media containing ESI are performed.

5. The Wisconsin court of appeals' analysis of petitioner's case was internally inconsistent.

The state court of appeals' analysis sometimes looked at the characteristics of an individual file, but at other times the court found petitioner's wife's authority to search the entire computer overrode the individual file characteristics:

- ¶31 (App:A13-A14): Without citing authority, the court of appeals found that petitioner's wife had authority over thumbcache image files which were inaccessible to her because petitioner didn't take measures to further restrict her ability to access them.

- ¶35 (App:A15-A16): The court of appeals found that petitioner's wife's authority to search the entire computer rendered her inability to access Inventory.doc (because it had been deleted by petitioner) irrelevant. Notably, petitioner had taken action to make the file inaccessible to her, so one wonders why the court of appeals bothered to make this a requirement in ¶31.

- ¶36 (App:A16): The court of appeals held that petitioner's wife's authority to search the entire computer overrode any privacy rights (as set forth in ***Rakas***, 439 U.S. at 143, n.12

and ***Randolph***, 547 U.S. at 111) petitioner had in Inventory.doc. In doing so, the court of appeals apparently found a search type to which ***Rakas*** and ***Randolph*** do not apply.

6. The solution is to generally disallow warrantless third party consent searches of media containing ESI.

"If police are to have workable rules, the balancing of the competing interests ... must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers." ***Riley***, 573 U.S. at 398 (internal citations omitted). This concept, coupled with the multiple issues created by carte blanche third party consent searches of media containing ESI, suggest the appropriate solution is to generally require police to obtain a warrant before conducting such a search. Otherwise, attempts to develop bounds around such unwarranted searches invariably will run into problems similar to those identified in ***Riley***, 573 U.S. at 398-401. Case in point is the state court of appeals' decision in the petitioner's case--this was an unqualified dragnet search of petitioner's life contained in the files on his computer, predicated upon his divorcing wife's "authority" over every single file on the computer, regardless of whether the file was private, confidential, privileged, password-protected, deleted, unknown to her, inaccessible to her, *or all of the above.*

The petitioner's circumstances highlight the importance of this Court granting review and deciding this issue. The Wisconsin court of appeals has issued a minimally-reasoned per curiam decision which found the petitioner's wife having actual (not apparent) common authority over ESI which the government knew was inaccessible to her. The petitioner cannot identify a single appellate decision in any jurisdiction with such a holding--the State certainly hasn't identified one. Yet, because ***Stone v Powell***, 428 U.S. 465, 493-95 (1976) precludes federal habeas review of a Fourth Amendment claim if the state courts have afforded a petitioner a full and fair hearing

on the matter, those in petitioner's shoes, where state courts seem to extrapolate Fourth Amendment law beyond reason, often have no recourse in federal court. Supreme Court review of this issue would eliminate the ambiguity in warrantless third party consent searches of media containing ESI, thus providing precise guidance from which state courts, in theory, cannot waver.

B. Social worker-patient privilege.

1. The Wisconsin courts placed a novel procedural requirement upon petitioner to prove social worker-patient privilege.

The petitioner invoked Wisconsin's social worker-patient privilege to: (1) show that his trial attorney provided ineffective assistance when he neglected to seek Inventory.doc's exclusion as evidence prior to petitioner pleading guilty, and (2) have petitioner's confidential information stricken from court records and other publicly-accessible records. The petitioner also invoked Wisconsin's privilege to have the court of appeals modify its decision to remove confidential information allegedly divulged to his family therapist. (Both "social workers" and "marriage and family therapists" are included in Wis. Stat. § 905.04--Privilege between certain health-care providers and patients.)

The State did not seriously oppose petitioner's claim of privilege regarding Inventory.doc because the State had agreed at sentencing that Inventory.doc was "an assignment[] for one of his sexual therapy classes that he had been in over the years" (R136:9-10) and therefore was judicially estopped from arguing against that position. ***State v. Ryan***, 2012 WI 16, ¶32, 338 Wis. 2d 695, 809 N.W.2d 37. Regardless, the circuit court sua sponte found petitioner's social

worker's affidavit (App:I01) insufficient, making a novel requirement that either the petitioner or his social worker had to testify to authenticate Inventory.doc:

> I do not have testimony from [the social worker] or anyone from his organization about [Inventory.doc] and whether it truly does fall under the social worker-patient privilege. I didn't even have any testimony by [petitioner] or any treatment provider regarding the origin of that document, why that document was created, when that document was created, the purpose for that document, the audience for that document.
>
> These are assertions, and for this Court to make a finding that it is a privileged document would require this Court to engage in speculation.

(R139:11-12; App:B58).

The petitioner's arguments to the court of appeals included an assertion that the Wisconsin Supreme Court's decision in ***Burch***, 398 Wis. 2d 1, supported petitioner's position (July 13, 2021 Letter; App:I01-I02). (Burch had argued that the State had insufficiently authenticated evidence by using an affidavit, but the Wisconsin Supreme Court found that the evidence was sufficiently authenticated by the affidavit according to Wis. Stat. § 909.02(12)--Self authentication of "Certified domestic records of regularly conducted activity." ***Id.*** at ¶34.)

The State had argued that petitioner did "not establish that 'inventory.doc' was privileged because [the affidavit from his social worker] d[id] not establish that the document was confidential" (Res. Br. 30). The court of appeals' decision merely parrotted the sua sponte proclamation of the circuit court with no analysis:

> We agree with the circuit court that [petitioner] failed to prove that the Inventory document was privileged under WIS. STAT. § 905.04(2). Neither [petitioner], the social worker, nor anyone else testified as to the circumstances surrounding the creation of the document, its purpose, or what steps were taken to preserve its confidentiality.

(App:A17-A18 (¶40)). Petitioner responded to the court of appeals' decision with a Motion for Reconsideration which pointed out that requiring live testimony was contrary to Wis. Stat. § 909.02(11)--Self authentication of "Patient health care records." (App:J01-J03). (Note that this is

the same statute cited in the ***Burch*** decision.) The petitioner also invoked Wis. Stat. § 905.04 in moving the court of appeals to modify its decision to remove confidential information allegedly divulged to his family therapist (App:K01-K03). The court of appeals denied both motions without analysis (App:A19). Petitioner made the same arguments in his petition for review to the Wisconsin Supreme Court which was denied without comment (App:C01).

2. Does this Court have jurisdiction?

On direct review of a state-court decision, this Court does not exercise jurisdiction if the state-court decision is clear on its face that it rests on an adequate and independent state-law ground. ***Michigan v. Long***, 463 U.S. 1032, 1040-41 (1983). However, "[n]ovelty in procedural requirements cannot be permitted to thwart review in this Court applied for by those who, in justified reliance upon prior decisions, seek vindication in state courts of their federal constitutional rights." ***N.A.A.C.P. v. Alabama ex rel. Patterson***, 357 U.S. 449, 457-58 (1958). The Wisconsin courts' sua sponte requirement of live testimony to authenticate Inventory.doc falls under the category of "novel procedural requirement" because it conflicts with Wisconsin statutes. Therefore, this Court can assert jurisdiction in petitioner's case.

3. Should federal social worker-patient privilege or state social worker-patient privilege be applied?

a. What is the federal privilege?

The federal social worker-patient privilege was formally established in ***Jaffee***, with this Court holding "that confidential communications between a licensed psychotherapist and her patients in the course of diagnosis or treatment are protected from compelled disclosure under Rule 501 of the Federal Rules of Evidence" and that "the federal privilege should also extend to

confidential communications made to licensed social workers in the course of psychotherapy." 518 U.S. at 15. This Court rejected a general balancing of the privilege when, "in the interests of justice, the evidentiary need for the disclosure of the contents of a patient's counseling sessions outweighs that patient's privacy interests" because "making the promise of confidentiality contingent upon a trial judge's later evaluation of the relative importance of the patient's interest in privacy and the evidentiary need for disclosure would eviscerate the effectiveness of the privilege." ***Id.***, 518 U.S. at 7, 17 (internal citation omitted). The privilege was not defined beyond the facts of ***Jaffee***, because "it is neither necessary nor feasible to delineate its full contours in a way that would govern all conceivable future questions in this area." ***Id.***, 518 U.S. at 18 (internal citation omitted).

b. Which psychotherapist-patient privilege should be used by federal courts in review of state criminal cases?

A review of nineteen state criminal cases brought to federal courts under 28 U.S.C. § 2254 (see Appendix N) shows federal courts usually rely on the state privilege statute to some degree, either entirely without ***Jaffee***, or in conjunction with ***Jaffee***. It seems appropriate to consider both federal and state privileges as over half of these decisions (53%) did so.

c. How should petitioner's case be decided?

Petitioner asserts that both the federal social worker-patient privilege and the Wisconsin privilege in Wis. Stat. § 905.04 should be used to evaluate whether Inventory.doc is privileged (and also whether one sentence included in the Wisconsin court of appeals' decision is privileged and should be stricken). Although the federal social worker-patient privilege was not defined completely in ***Jaffee***, subsequent lower court decisions have molded the federal privilege into the

facts of their cases. Some have gone back to the language in the 1972 amendment originally proposed to Congress but ultimately rejected in favor of the more open-ended Federal Rule of Evidence 501:

> We acknowledge that the Supreme Court Standard 504 is "a useful starting place" for an examination of this privilege... ***In re Bieter Co.***, 16 F.3d 929, 935 (8th Cir.1994).... As recommended by the Supreme Court in 1972, the Supreme Court Standard 504 provided that:
>
> A communication is "confidential" if not intended to be disclosed to third persons other than those present to further the interest of the patient in the consultation, examination, or interview, or persons reasonably necessary for the transmission of the communication, or persons who are participating in the diagnosis and treatment under the direction of the psychotherapist, including members of the patient's family.
>
> Supreme Court Standard 504(a)(3).
>
> ...
>
> In its general definition of the privilege, the Supreme Court Standard further provides:
>
> A patient has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications, made for the purpose of diagnosis or treatment of his mental or emotional condition, including drug addiction, among himself, his psychotherapist, or persons who are participating in the diagnosis or treatment under the direction of the psychotherapist, including members of the patient's family.
>
> Supreme Court Standard 504(b).

United States v. Ghane, 673 F.3d 771, 782-83 (8th Cir. 2012). *See also* ***Doe v. City of Chula Vista***, 196 F.R.D. 562, 565 (S.D. Cal. 1999).

This language is nearly the same as the Wisconsin privilege in Wis. Stat. § 905.04 (see Appendix D). Additionally, there are no exceptions in Wis. Stat. § 905.04 that would apply to petitioner's case, and the federal privilege does not generally apply balancing provisions, either (***Jaffee***, 518 U.S. at 7, 17). Therefore, it appears not to matter which privilege is applied in petitioner's circumstances--the end result will be the same. Should review be granted on this issue, petitioner will step through the Wisconsin privilege statute to show that (1) Inventory.doc

was privileged, (2) "there is a reasonable probability that, but for counsel's error[], he would not have pleaded guilty and would have insisted on going to trial," ***Hill v. Lockhart***, 474 U.S. 52, 59 (1985), and (3) therefore his attorney was ineffective for not seeking its exclusion.

4. Privileged and confidential information released should be stricken.

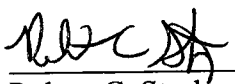
Petitioner contends the release of the confidential information contained in Inventory.doc violated his "constitutionally protected zone of privacy," which is derived from the "concept of ordered liberty" protected by the Fourteenth Amendment's Due Process Clause. ***Whalen v. Roe***, 429 U.S. 589, 598 (1977). He maintains an "individual interest in avoiding disclosure of personal matters." ***Id.***, 429 U.S. at 599.

Regardless which authority governs here, both the Wisconsin state privilege statute and federal privilege defined in ***Jaffee*** (using the 1972 language proposed to Congress) prevent *disclosure* of confidential communications. The information contained in Inventory.doc is unquestionably extremely personal, and the removal of references to it in court records and other publicly available documents is justified. *See e.g.*, ***Cobell v. Norton***, 213 F.R.D. 69, 77-79 (D. D.C. 2003) (ordering privileged and confidential information wrongfully obtained to be stricken from the court record). Similarly, petitioner is entitled to have the reference to a confidential communication allegedly revealed during a family counseling session to be removed from the court of appeals' decision.

CONCLUSION

The petition for a writ of certiorari should be granted for both issues because they concern inconsistent application of federal law by lower courts.

Respectfully submitted this first day of November, 2022,



Robert C. Stryker #650483
Pro se petitioner